UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/507,190	09/09/2004	Pim Theo Tuyls	NL 020192	1803

24737 7590 12/20/2007
PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
TRAORE, FATOUMATA	
ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
12/20/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/507,190	TUYLS ET AL.	
	Examiner	Art Unit	
	Fatoumata Traore	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 October 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *9-20* is/are rejected.

7)☒ Claim(s) *5-8* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the amendment filed on October 30th, 2007. Claims 17 and 18 have been amended; Claims 1-20 are pending and have been considered below.

Specification

2. In light of the amendment to the abstract, the objection to the abstract has been withdrawn.

Claim Rejections - 35 USC § 112

3. In light of the amendment to claim 17, the previous rejection of claims 17 and 18 has been withdrawn.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-20 are rejected under 35 U.S.C. 101 because: Claims to processes that do nothing more than solve mathematical problems manipulate abstract ideas or concepts are complex to analyze and are addressed herein. If the "acts" of a claimed process manipulate only numbers, abstract concepts or ideas, or signals representing any of the foregoing, the acts are not being applied to appropriate subject matter. Gottschalk v. Benson, 409 U.S. 63, 71 - 72, 175 USPQ 673,676 (1972). Thus, a process consisting solely of mathematical operations, i.e. converting one set of numbers into another set of numbers does not manipulate appropriate subject matter and thus cannot constitute a

statutory process. In practical terms, claims define nonstatutory processes if they:- consist solely of mathematical operations without some claimed practical application (i.e., executing a "mathematical algorithm"); or- simply manipulate abstract ideas, e.g., a bid (Schrader, 22 F.3d at 293-94, 3 USPQ2d at 1458-59) or a bubble hierarchy (Warmerdam, 33 F.3d at 1360, 31 USPQ2d at 1759), without some claimed practical application. Cf. Alappat, 33 F.3d at 1543 n~.19, 31 USPQ2d at t556 n.19 in which the Federal Circuit" recognized the confusion; The Supreme Court has not been clear.., as to whether such subject matter is excluded from the scope of 101 because it represents laws of nature, natural phenomena, or abstract ideas. See Diehr, 450 U.S. at 186 (viewed mathematical algorithm as a law of nature); Gottschalk v. Benson, 409 U.S. 63, 71-72 (1972) (treated mathematical algorithm as an "idea"). The Supreme Court also has not been clear as to exactly what kind of mathematical subject matter may not be patented. The Supreme Court has used, among others, the terms "mathematical algorithm," "mathematical formula," and "mathematical equation" to describe types of mathematical subject matter not entitled to patent protection standing alone. The Supreme Court has not set forth, however, any consistent or clear explanation of what it intended by such terms or how these terms are related, if at all. Certain mathematical algorithms have been held to be nonstatutory because they represent a mathematical definition of a law of nature or a natural phenomenon. For example, a mathematical algorithm representing the formula E = mc2 is a "law of nature" m it defines a "fundamental scientific truth" (~e., the relationship between energy and mass). To comprehend how the law of nature relates to any object, one invariably has to perform

certain steps (e.g., multiplying a number representing the mass of an object by the square of a number representing the speed of light). In such a case, a claimed process which consists solely of the steps that one must follow to solve the mathematical representation of E = mc2 is indistinguishable from the law of nature and would "preempt" the law of nature. A patent cannot be granted on such a process.

In addition, claim 19 is drawn to a computer program per se. Absent an explicit and deliberate definition in the specification or limiting claim language, the broadest reasonable interpretation of "computer program product" which would be fairly conveyed to one of ordinary skill in the art is a "produced computer program." A computer program is not a series of steps or acts and this is not a process. A computer program is not a physical article or object and as such is not a machine or manufacture. A computer program is not a combination of substances and therefore not a compilation of matter. Thus, a computer program by itself does not fall within any of the four categories of invention. Therefore, Claims 16-20 are not statutory.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1, 9-12, 16-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Leighton et al* (US 5519778) in view of Hoffstein et al (US 6076163).

Claims 1, 16, 17, 19: Leighton et al discloses a method, a system, a device, and a computer program product for of generating a private pair of key for enciphering communication between the users comprising:

A first party and a second party, in which the first party holds a value PI and a symmetrical polynomial P (x,y) fixed in the first argument by the value pl, and the first party performs the steps of sending the value pl to the second party(the individual secret keys allow two users I and j to easily agree on a common secret key Kij namely Kij = F(I, j). Pi and Qi constitute the secret of chip I) (column 4, lines 43-65), receiving a value P2 from the second party and calculating the common secret $1 by evaluating the polynomial P(pl, y) in P2, characterized in that the first party additionally holds a value ql and a symmetrical polynomial Q(x, z) fixed in the first argument by the value ql(this value is computed by user I evaluating the secret polynomial Pi at point j, and it is computed by user j evaluating the secret polynomial at Qj at point I) (column 4, lines 24-31 lines 43- 65, column 5 lines 5 lines 14-40 Figs. 1-3), but does not explicitly discloses the steps of sending ql to the second party, receiving a value q2 from the second party and calculating the secret $1 as SI=Q(ql, q2).P(PI, P2). However, Hoffstein et al discloses a secure user identification method, system, device and computer program product, which further discloses a step of sending ql to the second party (Fig. 3), a step of receiving a value 2 from the second party (Fig. 3) and a step of calculating the secret SI(column 3, lines 31-46 and Fig. 3). Therefore, it would have been obvious to one having ordinary skills in the art at the time the invention was made to use a challenge

response type of authentication in Leighton et al's disclosure. On would have been motivated to do so in order to maintain a secure communication by not allowing eavesdroppers to access critical information.

Claim 9: Leighton et al and Hoffstein et al disclose a method for of generating a private pair of key for enciphering communication between the users as in claim 1 above, and Leighton et al further discloses that the first party and the second party use a non-linear function on the generated secret S1 and S2, respectively, before using it as a secret key in further communications (n fact, the individual secret key assigned by T to user i consists of the two univariate polynomials P.sub.i =P.sub.i (y)=F(i,y) and Q.sub.i =Q.sub.i (x) =F(x,i). P.sub.i and Q.sub.i constitute the secret key of chip I) (column 4, lines 49-55).

Claim 10: Leighton et al and Hoffstein et al disclose a method for of generating a private pair of key for enciphering communication between the users as in claim 9 above, and Hoffstein et al further discloses that a one-way hash function is applied to the generated secrets S1 and S2(the above described user identification technique can be converted to a digital signature technique by the prover applying a one way hash function to Ag(x) to generate a simulated challenge polynomial) (column 3, lines 30-46). Therefore, it would have been obvious to one having ordinary skills in the art at the time the invention was made to use a hash function in Leighton et al's disclosure. On would have been motivated to do so in order to maintain a secure communication by not allowing eavesdroppers to access critical information.

Claim 11: Leighton et al and Hoffstein et al disclose a method for generating a private pair of key for enciphering communication between the users as in claim 9 above, and Leiflhton et al further discloses that the first party and the second party use a non-linear function on the generated secret S1 and S2, respectively, before using it as a secret key in further communications (n fact, the individual secret key assigned by T to user i consists of the two univariate polynomials P.sub.i =P.sub.i (y)=F(i,y) and Q.sub.i =Q.sub.i (x) =F(x,i). P.sub.i and Q.sub.i constitute the secret key of chip I) (column 4, lines 49-55).

Claim 12: Leighton et al and Hoffstein et al disclose a method for generating a private pair of key for enciphering communication between the users as in claim 1 above, and Hoffstein et al further discloses that a step of verifying that the second party knows the secret S1 (Fig. 3) (column 4, lines 49-55). Therefore, it would have been obvious to one having ordinary skills in the art at the time the invention was made to include a step of verifying that the second party knows the secret key in Leighton et al's disclosure. On would have been motivated to do so in order to authenticate the users.

Claim 18: Leighton et al and Hoffstein et al disclose a system for of generating a private pair of key for enciphering communication between the users as in claim 17 above, and Hoffstein et al further discloses a storage means for storing the polynomial P and the polynomial Q in the form their respective coefficients (Fig. 2B, item 30). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Leighton et al such as to include a storage means as

taught by Hoffstein et al. The motivation of doing so would have been maintaining data integrity.

7. Claims 2, 3, 4, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Leighton et al (US 5519778) in view of Hoffstein et al (US 6076163) in further view of Matyas et al (US 5953420).

Claim 2: Leighton et al and Hoffstein et al disclose a method for generating a private pair of key for enciphering communication between the users as in claim 1 above, while neither of them exclusive discloses a step of generating random numbers. However, Matyas et al discloses a method for establishing an authenticated shared secret value between a pair of users, which further discloses that the first party further performs the steps of obtaining a random number rl (user A generates a secret value Xla using a pseudorandom number generator) (column 6, lines 15-20), calculating .rl. ql (generates a public value Y1 from the secret value Xl as Y1 = G^xl mod p) (column 6 lines 20-25), sending rl .ql to the second party(each party transmits its own public value Y1 to the other party) (column 6, lines 35-38), receiving r2.q2 from the second party and calculating the secret $1 asSl=Q(ql, rl.r2.q2).P (pl, p2) (each party generates a value Z2 from the public value Y2 received from the other party and its own secret value X2.as Z2 =Y2^x2 mod p) (column 7, lines 33-45). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Leighton et al and Hoffstein et al such as to generate random

number in the secret key exchange protocol as taught by Matyas et al. The motivation of doing so would have been against attempts to retrieve the key.

Claim 3: Leighton et al, Hoffstein et al and Matyas et disclose a method for generating a private pair of key for enciphering communication between the users as in claim 2 above, and Matyas et al further discloses that the first party holds the Value ql multiplied by an arbitrarily chosen value r (user A generates a secret value Xla using a pseudorandom number generator) (column 6, lines 15- 20), and the product Q (ql, z). P (pl, y) instead of the individual polynomials P (pl, y) and Q (ql, z) (generatesa public value Y1 from the secret value Xl as Y1 = G^xl mod p) (column 6 lines 20-25), and the first party performs the steps of calculating rl .r.ql, sending rl.r.ql to the second party, receiving r2.r.q2 from the second party and calculating the secret S1 as S1= Q (ql, rl.r2.r.q2). P (pl, p2) (each party generates a value Z2 from the public value Y2 received from the other party and its own secret value X2 as Z2 =Y2^x2 mod p) (column 7, lines 33-45). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Leighton et al and Hoffstein et al such as to generate a Secret S1 as taught by Matyas et al. The motivation of doing so would have been against attempts to retrieve the key.

Claims 4, and 20: Leighton et al and Hoffstein et al disclose a method for generating a private pair of key for enciphering communication between the users as in claims 1 and 16 above, while above, while neither of them exclusive discloses a step of generating the secret key S2. However, Matyas et al discloses a method for establishing an authenticated shared secret value between a pair of users, which further discloses that

the second party holds a value P2 and a value q2(Fig. 4, item 400), the symmetrical polynomial P(x, y) fixed in the first argument by the value P2, the symmetrical polynomial Q(x, z) fixed in the first argument by the value q2, and the second party performs the steps of sending q2 to the first party(Fig.7 step 706), receiving ql from the first party (Fig. 7, step 708)and calculating a secret S2 as S2=Q(q2, ql)'P(P2, P1), whereby the common secret has been generated if the secret S2 equals the secret S1(each party generates a value Z2 from the public value Y2 received from the other party and its own secret value X2 as Z2 =Y2^x2 mod p) (column 7, lines 33-45). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Leighton et al and Hoffstein et al such as to generate a secret S1 as taught by Matyas et al. The motivation of doing so would have been against attempts to retrieve the key.

8. Claims 13-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Leighton et al (US 5519778) in view of Hoffstein et al (US 6076163) in further view of Menezes et al (handbook of applied Cryptography, ISBN 0-8493-8523-7 1997).

Claim 13:Leighton et al and Hoffstein et al disclose a method for generating a private pair of key for enciphering communication between the users as in claim 12 above, while neither of them explicitly a step of applying a zero knowledge protocol. However, Menezes et al discloses a similar method, which further discloses that the first party subsequently applies a zero-knowledge protocol to verify that the second party knows

the secret S1 (The prover claiming to be A selects a random element from pre-defined set as its secret commitment, and from this computes an associated (public) witness. This provides initial randomness for variation from other protocols runs, and essentially defines a set of questions all of which the prove claims to be able to answer, thereby a priori constraining her forthcoming response. By protocol design, only the legitimate party A, with knowledge of A's secret, is truly capable of answering all the questions, and the answer to any one of these provides no information about A's long-term Secret) (pages 409-410, section (IV)). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Leighton et al and Hoffstein et al such as to use a zero-knowledge protocol as taught by Menezes et al. The motivation of doing so would have been providing unconditional security.

Claim 14:Leighton et al and Hoffstein et al disclose a method for generating a private pair of key for enciphering communication between the users as in claim 12 above, while neither of them explicitly a step of applying a commitment- based protocol and Menezes et al discloses a similar method, which further discloses that the first party subsequently applies a commitment-based protocol to verify that the second party knows the secret S1 (*The prover claiming to be A selects a random element from pre-defined set as its secret commitment, and from this computes an associated (public) witness. This provides initial randomness for variation from other protocols runs, and essentially defines a set of questions all of which the prove claims to be able to answer, thereby a priori constraining her forthcoming response. By protocol design, only the*

legitimate party A, with knowledge of A's secret, is truly capable of answering all the questions, and the answer to any one of these provides no information about A's long-term secret) (pages 409-410, section (IV)). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Leighton et al and Hoffstein et al such that to use a commitment based protocol as taught by Menezes et al. The motivation of doing so would have been providing unconditional security.

Claim 15: Leighton et al and Hoffstein et al disclose a method for generating a private pair of key for enciphering communication between the users as in claim 14 above, while neither of them explicitly a step of using a symmetric cipher to encrypt a random challenge. However, Menezes et al disclose a similar method which, further discloses that the second party uses a symmetric cipher to encrypt a random challenge (*b chooses a random r, computes the witness x = h(r) (x demonstrates knowledge of r without disclosing it and computes the challenge e = PA(r, B)) (page 404, section (I))*, and sends the encrypted random challenge to the first party(*B sends the encrypted random challenge to A. A decrypts e to recover r' and B' computes x' = h (r') (page 404, section (I)* and the first party subsequently uses the same symmetric cipher as a commit function to commit himself to a decryption of the encrypted random challenge (*A sends r= r' to B. B succeeds with unilateral entity authentication of A upon verifying) (page 404, section (I))*. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Leighton et al

and Hoffstein et al such as to use a symmetric cipher as taught by Menezes et al. The motivation of doing so would have been providing unconditional security.

Allowable Subject Matter

9. Claims 5-8 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Response to Arguments

10. Applicant's arguments filed June 4th, 2007 regarding the 101 rejection previously withdrawn by the examiner have been fully considered but they are not persuasive.

11. As stated in the Non-Final Rejection dated February 27th, 2007 and the above rejection, one may not patent every "substantial practical application" of an idea, law of nature or natural phenomena because such a patent "in practical effect be a patent on the [idea, law of nature or natural phenomena] itself." Gottschalk v. Benson, 409 U.S. 63, 71-72, 175 USPQ 673, 676 (1972).

12. The claims in Gottschalk were directed to a mathematical method running on a computer: converting binary-coded-decimal (BCD) numerals into pure binary numerals for use with general purpose digital computer of any type. Gottshcalk at 65.

13. The Supreme Court held in Gottschalk that "one may not patent an idea. But in practical effect that would be the result if the formula for converting BCD numerals to

pure binary numerals were patented in this case. The mathematical formula involved here has no substantial practical application except in connection with a digital computer, which means that if the judgment below is affirmed, the patent would wholly pre-empt the mathematical formula and in practical effect would be a patent on the algorithm itself." Gottshcalk at 71-72.

14. Therefore, whether a claim recites a machine implemented process is not determinative of whether that process claim is statutory. Thus, a claim that is nothing more than a machine-implemented abstract idea is invalid.

15. Moreover, the Supreme Court also held that "[h]ere the 'process' claim is so abstract and sweeping as to cover both known and unknown uses of the BCD to pure binary conversion. The end use may (1) vary from the operation of a train[,] to verification of drivers' licenses[,] to researching the law books for precedents[;] and (2) be performed through any existing machinery or future- devised machinery or without any apparatus." Gottshcalk at 68.

16. The Examiner finds that the claims in the instant application share the same characteristics as the claims in Gottshcalk. The claims in the instant application are directed to a machine-implemented abstract idea. These claims are: (1) so abstract and sweeping as to cover both known and unknown uses of the underlying math, (2) so abstract and sweeping as to be applicable to a wide variety of unrelated applications.

17. For example, independent claim 1 recites "A method of generating a common secret between a first party and a second party, in which the first party holds a value PI and a symmetrical polynomial P(x,y) fixed in the first argument by the value pI, and the

first party performs the steps of sending the value p~ to the second party, receiving a value P2 from the second party and calculating the common secret S~ by evaluating the polynomial P(p~, y) in P2, characterized in that the first party additionally holds a value q~ and a symmetrical polynomial Q(x, z) fixed in the first argument by the value ql, and further performs the steps of sending q~ to the second party, receiving a value q2 from the second party and calculating the secret $1 as Sl=Q(ql, q2).P(Pl, P2)"

18. Claim 1 does not include any practical applications for generating a common secret between parties. However, applicant argued on page 8 of the March 2nd reply that" the specification includes example practical applications for generating a common secret between parties, including the use of "Chip In Disk" (CID) products that descramble information on a disk only when the receiving device is authenticated"

19. First, Applicant is respectfully reminded that during patent examination, the pending claims must be "given their broadest reasonable interpretation consistent with the specification." (Phillips v. AWH Corp., 415 F.3d 1303, 75 USPQ2d 1321 (Fed. Cir. 2005)). See MPEP 2111.

20. In that regard, the court explained that "reading a claim in light of the specification, to thereby interpret limitations explicitly recited in the claim, is a quite different thing from reading limitations of the specification into a claim,' to thereby narrow the scope of the claim by implicitly adding disclosed limitations which have no express basis in the claim." See MPEP 2111, In re Prater, 415 F.2d 1393, 1404- 05, 162 USPQ 541,550-51 (CCPA 1969), and also In re Morris, 127 F.3d 1048, 1054-55, 44 USPQ2d 1023, 1027-28 (Fed. Cir. 1997).

21. Therefore, the examiner respectfully maintains the rejection of claims 1-20 under 35 U.S.C. 101.

22. Applicant's arguments filed October 30th, 2007 have been fully considered but they are not persuasive.

Applicant argued that on page 10 of the reply that "Because neither Leighton nor Hoffman, individually or collectively, teaches or suggests generating a common secret between a first party and a second party as a product of two symmetrical polynomials that are each evaluated in a value received from the second party,"

In reply, the examiner respectfully disagrees and submits that the above future is taught by Hoffstein et al (See Fig. 5, steps, 1-4; also see column 3, lines 45-65).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571) 270-1685. The examiner can normally be reached Monday through Thursday from 7:00 a.m. to 4:00 p.m. and every other Friday from 7:30 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nassar G. Moazzami, can be reached on (571) 272 4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is (571) 273-8300. Draft or Informal faxes, which will not be entered in the application, may be submitted directly to the examiner at (571) 270-2685.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

FT
Tuesday December 18th, 2007

Nassar G. Moazzami
Supervisory Patent Examiner

12/19/07